DETAILED ACTION

1. This action is in response to the telephone interview initiated by Examiner on 04/10/2008.

2. Claims 11- 24 are pending for consideration.

EXAMINER'S AMENDMENT

3. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Ed Garcia on 04/10/2008.

The application has been amended as follows:

Cancel claims 1-10 and 22-23.

Amend claims 11, 21 and 24.

Claim 11:

A method for generating a public key certificate of an end entity by a registration authority and an issuing authority in a public key infrastructure, comprising the steps of:

generating, by the registration authority, a signature to contents to be registered with a public key certificate having its own valid term, and a certificate issuing request

including both the contents signed by the registration authority and a signature to the contents signed by the registration authority; -

sending the certificate issuing request from the registration authority to the issuing authority;

generating, in response to the certificate issuing request, by the issuing authority, a public key certificate including the contents signed by the registration authority, the signature to the contents signed by the registration authority, issuing contents to be issued by the issuing authority, and an issuing authority signature to the contents signed by the registration authority, the signature to the contents signed by the registration authority and the issuing contents issued by the issuing authority; [[and]]

sending the public key certificate from the issuing authority to the registration authority for being registered within the registration authority;

deleting information, at the registration authority, on the public key certificate having been generated if the valid term has been ended; and

deleting information, at the registration authority, on the public key certificate having been generated in response to a public key certificate invalidation request sent from the issuing authority.

Claim 21:

A certificate authority to be used in a public key infrastructure including a plurality of end entities comprising:

(A) a registration authority for ~~generating~~:

(A-1) generating a signature to contents to be registered with a public key certificate having its own valid term, of each of the plurality of end entities; and

(A-2) generating a certificate issuing request including both the contents signed by the registration authority and a signature to the contents signed by the registration authority; and

(A-3) deleting information, at the registration authority, on the public key certificate having been generated if the valid term has been ended; and

(A-4) deleting information, at the registration authority, on the public key certificate having been generated in response to a public key certificate invalidation request sent from [[the]] an issuing authority; and

(B) [[an]] the issuing authority [[(12)]] connected to the registration authority through a network for generating, in response to the certificate issuing request, a public key certificate including:

(B-1) the contents signed by the registration authority;

(B-2) the signature to the contents signed by the registration authority;

(B-3) issuing contents to be issued by the issuing authority; and

(B-4) an issuing authority signature to the contents signed by the registration authority, the signature to the contents signed by the registration authority and the issuing contents issued by the issuing authority, the public key certificate being sent to the registration authority and registered within the registration authority.

Claim 24:

A method for generating a public key certificate of an end entity by a registration authority and an issuing authority in a public key infrastructure, comprising the steps of:

generating, by the registration authority, a signature to contents to be registered with a public key certificate having its own valid term, and a certificate issuing request including both the contents signed by the registration authority and a signature to the contents signed by the registration authority; -

sending the certificate issuing request from the registration authority to the issuing authority;

generating, in response to the certificate issuing request, by the issuing authority, a public key certificate including the contents signed by the registration authority, the signature to the contents signed by the registration authority, issuing contents to be issued by the issuing authority, and an issuing authority signature to the contents signed by the registration authority, the signature to the contents signed by the registration authority and the issuing contents issued by the issuing authority;

sending the public key certificate from the issuing authority to the registration authority for being registered within the registration authority;

deleting information, at the registration authority, on the public key certificate having been generated if the valid term has been ended; and

deleting information, at the registration authority, on the public key certificate having been generated in response to a public key certificate invalidation request sent from the issuing authority.

Allowable Subject Matter

4. Claims 11-21 and 24 are allowed.

5. The following is an examiner's statement of reasons for allowance:

The claimed invention concerns about "a problem that the responsibility ranges of the issuing authority and the registration authority are not clear, although their responsibility ranges are defined by the Certificate Practice Statement. However, when a problem arises in issued public key certificate, internal data of the issuing authority and the registration authority should be checked to determine who is responsible" (See page 4 lines 8-17 of Applicant's specification).

The closes prior art, Matsuyama, discloses the method of requesting and issuing public key certificate by a registration authority and a certificate authority. Matsuyama further discloses "generating, by the registration authority, a signature to contents to be registered with a public key certificate (Matsuyama: see figure 16A and lines 24-34 of column 20), and a certificate issuing request including both the contents signed by the registration authority and a signature to the contents signed by the registration authority (Matsuyama: see figures 16A and 19, column 3 lines 22-40 and column 22 lines 15-67 and column 23 lines 1-5)" and "sending the certificate issuing request from the registration authority to the issuing authority (Matsuyama: see figure 16A and column 22 lines 64-67 and column 23 lines 1-5)". However, Matsuyama fails to disclose the following limitations "generating, in response to the certificate issuing request by the issuing authority, a public key certificate including the contents signed by the

registration authority, the signature to the contents signed by the registration authority, issuing contents to be issued by the issuing authority, and an issuing authority signature to the contents signed by the registration authority, the signature to the contents signed by the registration authority and the issuing contents issued by the issuing authority; and sending the public key certificate from the issuing authority to the registration authority for being registered within the registration authority" and "wherein the public key certificate having been generated includes its own valid term, and wherein the registration authority is arranged to delete information on the public key certificate if the valid term has been ended."

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled “Comments on Statement of Reasons for Allowance.”

Any inquiry concerning this communication or earlier communications from the examiner should be directed to TRANG DOAN whose telephone number is (571)272-0740. The examiner can normally be reached on Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Trang Doan/
Examiner, Art Unit 2131

/Christopher A. Revak/
Primary Examiner, Art Unit 2131